Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ASCT 2600

E-mail: pjcis@aph.gov.au

Submission from the Uniting Church in Australia, Synod of Victoria and Tasmania to the review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

1 July 2019

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to make a submission to the review on the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

The Synod continues to be of the view that the Australian Parliament should not rely on ICT corporations to voluntarily co-operate with law enforcement, even in the most serious cases of murder, terrorism and the rape and torture of children. The Parliament needs to ensure Australia's laws are able to compel timely co-operation with appropriate oversight, safeguards and accountability of the law enforcement agencies.

The Synod would urge that the Committee to ensure that ICT businesses are excluded by law from being moderators of law enforcement activity. To the extent that law enforcement activities are limited and restrained, it should be by judicial oversight and not by ICT businesses having the ability to contest legitimate law enforcement activities.

Processes to compel co-operation from ICT corporations should be as expeditious as is reasonably possible, not requiring a court issued warrant for every request. Court issued warrants should be for accessing the content of personal communications. Forcing law enforcement agencies to get a warrant from a court every time they want to access any sort of data about a person for an investigation, such as matching the IP address of someone accessing child sexual abuse material, to an actual person slows down police investigations. The Australian Federal Police have far too many online child sexual abuse cases to deal with already. Tying them up in unnecessary red tape will mean that some children who could be rescued from further sexual or other physical abuse will continue to suffer such abuse and will leave more perpetrators of such abuse free to continue in their behaviour for longer before they are eventually caught and dealt with. Against that, there is a line to be walked to ensure that Australia does not become a police state, but we remain a long way from that point.

Multinational ICT corporations have been able to act as intermediaries between law enforcement agencies and the information people place online, having the power to decide how easy or difficult it will be for law enforcement agencies to access that information. This is a substantial transfer of power away from law enforcement agencies, which are accountable to an elected government, and an independent judiciary and into the hands of multinational corporations that have a demonstrated history of playing fast and loose with national laws when it suits them, as demonstrated by the complex artificial arrangements entered into to

avoid paying tax in the places where people are accessing their services or making purchases.

As pointed out by Professor Alan Rozenshtein, these corporations hold a large degree of discretion when processing requests from law enforcement agencies: discretion in being able to slow down the processing of requests by insisting on proceduralism and in minimising their capacity to respond to legal requests by implementing encryption.[1]

This discretion means these corporations determine, at least in part, government agencies access to information about our personal relationships, professional engagements, travel patterns and financial circumstances. At the same time, they impact on government's ability to prevent terrorism, the rape of children, solve murders and locate missing children. These corporations are now responsible for decisions that have major consequences for our privacy on the one hand, and our safety and well-being on the other.[2] Ultimately, these should be decisions for democratically elected governments, who are accountable to citizens, rather than multinational corporations that ultimately are accountable to shareholders whose main concern is the maximisation of profit.

The Harvard Law Review notes there are a variety of factors that result in multinational ICT corporations co-operating or obstructing law enforcement agencies and challenging court orders. Amongst these are if resisting a court order will boost or protect the reputation of the corporation amongst users of its technology, which in turn will increase sales and profits.[3]

Since our previous submission to the Committee, *The Financial Times* reported that videos and images of children being sexually abused were being openly shared on Facebook's WhatsApp on a vast scale.[4] Israeli researchers warned Whatsapp that it was easy to find and join dozens of chat groups where people were sharing images and videos of children being sexually abuses. In one case, one of these groups had 256 members.

Google reserves the right to tip off an alleged offender they are under investigation, unless forbidden from doing so by a court order. Google's policy statement indicates that Google will inform a user when law enforcement has made a request to access their data, unless the law prohibits the user being notified, as stated under Googles' policy:[5]

> *If Google receives ECPA legal process for a user's account, it's our policy to notify the user via email before any information is disclosed unless such notification is prohibited by law. We will provide delayed notice to users after a legal prohibition is lifted, such as when a statutory or court ordered gag period has expired. We might not give notice when, in our sole discretion, we believe that notice would be counterproductive or exceptional circumstances exist involving danger of death or serious physical injury to any person. In such cases, we will provide delayed notice if we later determine that those circumstances no longer exist. In cases where the account in question is an enterprise hosted account, notice may go to the domain administrator, or the end user, or both.*

---

[1] 'Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance', *Developments in Law – More Data, More Problems,* 131 Harvard Law Review (2018), 1715-1722.
[2] 'Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance', *Developments in Law – More Data, More Problems,* 131 Harvard Law Review (2018), 1715-1722.
[3] 'Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance', *Developments in Law – More Data, More Problems,* 131 Harvard Law Review (2018), 1715-1722.
[4] Leila Abboud, Hannah Kuchler and Mehul Srivastava, 'WhatsApp fails to curb sharing of child sex abuse videos', *The Financial Times,* 20 December 2018, https://www ft.com/content/bff119b8-0424-11e9-99df-6183d3002ee1
[5] https://support.google.com/transparencyreport/answer/7381738?hl=en&ref_topic=7380433

This policy would appear to create the risk, except where a court order prohibits it, Google may tip off criminals that they are under investigation and maximises their opportunity to destroy evidence or take flight.

In correspondence to the Uniting Church from the Security Counsel of the Child Safety Team of Google on this point, Google stated:[6]

> *Google may notify a user before information about them is disclosed unless such notification is prohibited by law or in cases involving a danger of death or serious bodily injury to a person, including children. Our policy also highlights that "If the request appears to be legally valid, we will endeavour to make a copy of the requested information before we notify the user."*

This raises a number of questions about how Google is qualified to assess if tipping off a user they are under investigation by police will involve the risk of someone being murdered or subject to serious bodily injury. What do Google staff define as serious bodily injury? What about emotional or mental harms that may result on a victim or victims from the alleged offender being tipped off? The preservation of the requested information also ignores that being tipped off may allow the alleged offender to destroy evidence that is not covered by the legal request from the law enforcement agency, which may include platforms that Google has no control or oversight over.

[redacted]
Senior Social Justice Advocate
Synod of Victoria and Tasmania
Uniting Church in Australia
29 College Crescent
Parkville Victoria 3052
[redacted]

[6] Correspondence from Security Counsel, Child Safety Team, Google, to the Uniting Church in Australia, 17 June 2019.